Control Plane Policing

The Control Plane Policing feature allows you to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Restrictions for Control Plane Policing

Input Rate-Limiting Support

Input rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to input control plane traffic with the **service-policy input** command. For more information, see the “Input Rate-Limiting and Silent Mode Operation” section.

MQC Restrictions

The Control Plane Policing feature requires the Modular QoS CLI (MQC) to configure packet classification and traffic policing. All restrictions that apply when you use the MQC to configure traffic policing also apply when you configure control plane policing.

Match Criteria Support

Only the extended IP access control lists (ACLs) classification (match) criteria is supported.

Restrictions for CoPP on the RSP3

- sdm prefer enable_copp template must be enabled on the the RSP3 module to activate COPP.
- Ingress and Egress marking are not supported.
- Egress COPP is not supported. COPP with marking is not supported.
- CPU bound traffic (punted traffic) flows is supported via the same queue with or without CoPP.
- Only match on access group is supported on a CoPP policy.
- Hierarchical policy is not supported with CoPP.
- Class-default is not supported on CoPP policy.
- User defined ACLs are not subjected to CoPP classified traffic.
- A CoPP policy map applied on a physical interface is functional.
- When COPP template is enabled, classification on outer Vlan, inner Vlan, Inner Vlan Cos, destination MAC address, source IP address, and destination IP address are not supported.

  The template-based model is used to enable COPP features and disable some of the above mentioned QOS classifications.
- When sdm prefer enable_copp template is enabled, sdm prefer enable_match_inner_dscp template is not supported.
- Only IP ACLs based class-maps are supported. MAC ACLs are not supported.
- Multicast protocols like PIM, IGMP are not supported.
- Only CPU destined Unicast Layer3 protocols packets are matched as part of COPP classification.

Restrictions on Firmware

- Port ranges are not supported.
- Only exact matches are supported, greater than, less than and not equal are not supported.
- Internet Control Message Protocol (ICMP) inner type’s classification not supported.
- Match any is only supported at class-map level.
- Policing action is supported on a CoPP policy map.

Information About Control Plane Policing

Benefits of Control Plane Policing

Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

Control Plane Terms to Understand

On the router, the following terms are used for the Control Plane Policing feature:

- Control plane—A collection of processes that run at the process level on the Route Processor (RP). These processes collectively provide high-level control for most Cisco IOS XE functions. The traffic sent to or sent by the control plane is called control traffic.
- Forwarding plane—A device that is responsible for high-speed forwarding of IP packets. Its logic is kept simple so that it can be implemented by hardware to do fast packet-forwarding. It punts packets that require complex processing (for example, packets with IP options) to the RP for the control plane to process them.

Control Plane Policing Overview

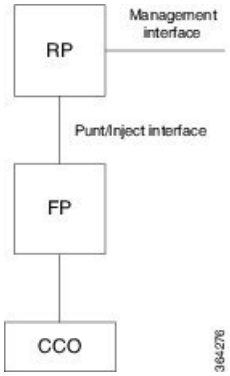
To protect the control plane on a router from DoS attacks and to provide fine-control over the traffic to the control plane, the Control Plane Policing feature treats the control plane as a separate entity with its own interface for ingress (input) and egress (output) traffic. This interface is called the punt or inject interface, and it is similar to a physical interface on the router. Along this interface, packets are punted from the forwarding plane to the RP (in the input direction) and injected from the RP to the forwarding plane (in the output direction). A set of quality of service (QoS) rules can be applied on this interface (in the input direction) in order to achieve CoPP.

These QoS rules are applied only after the packet has been determined to have the control plane as its destination. You can configure a service policy (QoS policy map) to prevent unwanted packets from progressing after a specified rate limit has been reached; for example, a system administrator can limit all TCP/TELNET packets that are destined for the control plane.

You can use the **platform qos-feature copp-mpls enable** command to enable the Control Plane Policing feature on the device for MPLS explicit null scenario, control packets destined to the device is punted to proper control CPU Q. If CoPP-MPLS remains disabled, then self destined control packets like BGP, LDP, telnet and so on, that are MPLS explicit null tagged are not classified by CoPP and is punted to HOST_Q instead of CFM_Q/CONTROL_Q.

Note The command **platform qos-feature copp-mpls enable** is supported only on Cisco NCS 4200 platform.

Figure 1: Abstract Illustration of a Router with a Single RP and Forwarding Plane



The figure provides an abstract illustration of the router with a single RP and forwarding plane. Packets that are destined to the control plane come in through the carrier card and then go through the forwarding plane before being punted to the RP. When an input QoS policy map is configured on the control plane, the forwarding plane performs the QoS action (for example, a transmit or drop action) before punting packets to the RP in order to achieve the best protection of the control plane in the RP.

Note As mentioned in this section, the control plane interface is directly connected to the RP, so all traffic through the control plane interface to or from the control-plane is not subject to the CoPP function performed by the forwarding plane.

Supported Protocols

The following table lists the protocols supported on Control Plane Policing feature.

Supported Protocols	Criteria	Match	Queue#
TFTP - Trivial FTP	Port Match	IP access list ext copp-system-acl-tftp permit udp any any eq 69	NQ_CPU_HOST_Q
TELNET	Port Match	IP access list ext copp-system-acl-telnet permit tcp any any eq telnet	NQ_CPU_CONTROL_Q
NTP - Network Time Protocol	Port Match	IP access list ext copp-system-acl-ntp permit udp any any eq ntp	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
FTP - File Transfer Protocol	Port Match	IP access list ext copp-system-acl-ftp permit tcp host any any eq ftp	NQ_CPU_HOST_Q
SNMP - Simple Network Management Protocol	Port Match	IP access list ext copp-system-acl-snmp permit udp any any eq snmp	NQ_CPU_HOST_Q
TACACS - Terminal Access Controller Access-Control System	Port Match	IP access list ext copp-system-acl-tacacs permit tcp any any tacacs	NQ_CPU_HOST_Q
FTP-DATA	Port Match	IP access list ext copp-system-acl-ftpdata permit tcp any any eq 20	NQ_CPU_HOST_Q
HTTP - Hypertext Transfer Protocol	Port Match	IP access list ext copp-system-acl-http permit tcp any any eq www	NQ_CPU_HOST_Q
WCCP - Web Cache Communication Protocol	Port Match	IP access list ext copp-system-acl-wccp permit udp any eq 2048 any eq 2048	NQ_CPU_HOST_Q
SSH - Secure Shell	Port Match	IP access list ext copp-system-acl-ssh permit tcp any any eq 22	NQ_CPU_HOST_Q
ICMP - Internet Control Message Protocol	Protocol Match	IP access list copp-system-acl-icmp permit icmp any any	NQ_CPU_HOST_Q
DHCP - Dynamic Host Configuration Protocol	Port Match	IP access list copp-system-acl-dhcp permit udp any any eq bootps	NQ_CPU_HOST_Q
MPLS- OAM	Port Match	IP access list copp-system-acl-mplsoam permit udp any eq 3503 any	NQ_CPU_HOST_Q

Supported Protocols	Criteria	Match	Queue#
LDP - Label Distribution Protocol	Port Match	IP access list copp-system-acl-ldp permit udp any eq 646 any eq 646 permit tcp any any eq 646	NQ_CPU_CFM_Q
RADIUS - Remote Authentication Dial In User Service	Port Match	IP access list copp-system-radius permit udp any any eq 1812 permit udp any any eq 1813 permit udp any any eq 1645 permit udp any any eq 1646 permit udp any eq 1812 any permit udp any eq 1813 any permit udp any eq 1645 any	NQ_CPU_HOST_Q

Input Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure input policing on control plane traffic using the **service-policy input** *policy-map-name* command.

Rate-limiting (policing) of input traffic from the control plane is performed in silent mode. In silent mode, a router that is running Cisco IOS XE software operates without receiving any system messages. If a packet that is entering the control plane is discarded for input policing, you do not receive an error message.

How to Use Control Plane Policing

Defining Control Plane Services

Perform this task to define control plane services, such as packet rate control and silent packet discard for the RP.

Before you begin

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Input policing does not provide any performance benefits. It simply controls the information that is entering the device.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **control-plane**

Example:

```
Device(config)# control-plane
```

Enters control-plane configuration mode (which is a prerequisite for defining control plane services).

Step 4 **service-policy** [**input** |**output**] *policy-map-name*

Example:

```
Device(config-cp)# service-policy input control-plane-policy
```

Attaches a QoS service policy to the control plane.

- **input**—Applies the specified service policy to packets received on the control plane.
- *policy-map-name*—Name of a service policy map (created using the **policy-map** command) to be attached.

Step 5 **end**

Example:

```
Device(config-cp)# end
```

(Optional) Returns to privileged EXEC mode.

Verifying Control Plane Services

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show policy-map control-plane** [**all**] [**input** |**output** [**class** *class-name*]]

Example:

```
Device# show policy-map control-plane all
```

Displays information about the control plane.

- **all**—(Optional) Displays service policy information about all QoS policies used on the CP.
- **input**—(Optional) Displays statistics for the attached input policy.
- **class** *class-name*—(Optional) Specifies the name of the traffic class whose configuration and statistics are displayed.

Step 3 **exit**

Example:

```
Device# exit
```

(Optional) Exits privileged EXEC mode.

Examples

The following example shows that the policy map TEST is associated with the control plane.

Configuring Control Plane Policing to Mitigate Denial-of-Service Attacks

Apply control plane policing (CoPP) to ICMP packets to mitigate denial of service (DoS) attacks.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

Step 2 **configure terminal**

Example:

```
Device# configure terminal
```

Enters global configuration mode.

Step 3 **access-list** *access-list-number* **permit** *protocol* {**tcd | udp**} {**any | host** {*source-addr* | *name*}} **eq** *port number* {**any | host** {*source-addr* | *name*}} **eq** *port number*

Example:

Configures an access list for filtering frames by UDP protocol and matches only packets with a given port number.

Step 4 **class-map [match-any | match-all | type]** *class-map-name*

Example:

```
Device(config)# class-map match-any MyClassMap
```

Creates a class-map and enters QoS class-map configuration mode.

Step 5 **match access-group** [*access-list-index* | *access-group-name*]

Example:

```
Device(config-cmap)# match access-group 111
```

Specifies access groups to apply to an identity policy. The range of valid values is 1-2799.

Step 6 **exit**

Example:

```
Device(config-cmap)# exit
```

Exits QoS class-map configuration mode and returns to global configuration mode.

Step 7 **policy-map** *policy-map-name*

Example:

```
Device(config)# policy-map Policy1
```

Specifies a service policy and enters QoS policy-map configuration mode.

Step 8 **class** [*class-map-name* | *class-default*]

Example:

```
Device(config-pmap)# class MyClassMap
```

Enters QoS policy-map class configuration more

Step 9 **police** {*rate-bps* | **cir** {*cir-bps* | **percent** *percent*}} [**bc** *burst-bytes*] [**conform-action** | **exceed-action** | **violate-action**]*action*] [ ]

Example:

Configure a traffic policer based on the traffic rate or committed information rate (CIR). By default, no policer is defined.

- *rate-bps*—Specifies average traffic rate in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **cir**—Specifies a committed information rate (CIR).
- *cir-bps*—Specifies a CIR in bits per second (b/s). The range is 64000 to 10000000000. Supply an optional postfix (K, M, G). Decimal point is allowed.
- **be** *burst-bytes*—(Optional) Specifies the conformed burst (be) or the number of acceptable burst bytes. The range is 8000 to 16000000.
- **conform-action** *action*— (Optional) Specifies action to take on packets that conform to the specified rate limit.
- **pir** *pir-bps*—(Optional) Specifies the peak information rate (PIR).

Note **cir percent** *percent* option is not supported on the router.

Step 10 **exit**

Example:

```
Device(config-pmap-c-police)# exit
```

Exits policy-map class police configuration mode

Step 11 **exit**

Example:

```
Device(config-pmap-c)# exit
```

Exits policy-map class configuration mode

Step 12 **exit**

Example:

```
Device(config-pmap)# exit
```

Exits policy-map configuration mode

Step 13 **control-plane**

Example:

```
Device(config)# control-plane
```

Enters control plane configuration mode.

Step 14 **service-policyinput** *policy-map-name*

Example:

```
Device(config-cp)# service-policy input Policy1
```

Attaches a policy map to a control plane.

Step 15 **exit**

Example:

```
Device(config-cp)# exit
```

Exits control plane configuration mode and returns to global configuration mode.

Step 16 **exit**

Example:

```
Device(config)# exit
```

Exits global configuration mode returns to privileged EXEC mode.

Configuration Examples for Control Plane Policing

Example: Configuring Control Plane Policing on Input Telnet Traffic

Verification Examples for CoPP

The following example shows how to verify control plane policing on a policy map.

```
Router# show policy-map control-plane
           Control Plane
         Service-policy input: control-plane-in
         Class-map: telnet-class (match-all)
           10521 packets, 673344 bytes
           5 minute offered rate 18000 bps, drop rate 15000 bps
           Match: access-group 102
           police:  cir 64000 bps, bc 8000 bytes
           conformed 1430 packets, 91520 bytes; actions:
           transmit
           exceeded 9091 packets, 581824 bytes; actions:
           drop
          conformed 2000 bps, exceeded 15000 bps
     Class-map: class-default (match-any)
           0 packets, 0 bytes
           5 minute offered rate 0000 bps, drop rate 0000 bps
          Match: any
```

The following command is used to verify the TCAM usage on the router.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html

Standards and RFCs

Standard/RFC	Title
No specific Standards and RFCs are supported by the features in this document.	—

MIBs

MIB	MIBs Link
—	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html